The Indian Information Technology Act and Spamming

Journal of Internet Banking and Commerce, April 2006, vol. 11, no.1
(http://www.arraydev.com/commerce/jibc/)

By Rahul Goel, Advocate

Web: http://www.goel.co.in
Email: rahul@goel.co.in

Mr. Rahul Goel is licensed to practice as an Advocate in India. Presently, he is associated with Seth Dua & Associates, Solicitors & Advocates, India. He qualified as a software engineer before going onto undertake further studies in law. He completed his LL.M in Information Technology, Media and E-Commerce law at University of Essex, UK. His practice focuses on Technology & Telecommunication laws, Competition laws, Regulatory Affairs, Intellectual Property laws, E-Commerce and WTO laws.

Abstract

The article makes an attempt to analyse provisions relating to privacy especially spamming and phishing in the proposed amendments to the Indian Information Technology Act, 2000.

Today, the technology is the driving force of any economy. However, to check that such driving force follows the path of law and works in larger interest of the society, all countries need a robust legislation. Internet is one such technology, which spans across the globe, out of direct control of any single country or legislation. The countries like United States and United Kingdom have enacted legislations to safeguard the interests of their citizens and traders. India enacted its first legislation, the Information Technology Act, 2000 to regulate Internet and e-commerce in 2000. However, as technology evolved, the offences in this area took a different path and the provisions of the existing legislation were found to be ineffective in curbing such crimes.

A couple of isolated cases of theft relating to confidential data of the client from BPOs/ call centers rocked the entire information technology sector in India. It was soon realized that the existing Act needs to be amended to include provisions relating to misuse of evolved technology. The Government of India with an aim to amend the Information technology Act, 2000 constituted an Expert Committee. The Committee after reviewing several issues including issues relating to privacy and protection of data has recently submitted its recommendations and suggestions to the Government of India.

The Committee has made an attempt to address issues relating to electronic contracts, breach

of confidentiality and privacy, child pornography, electronic/ digital signatures etc. However, the recommendations are silent on prosecution as regard to phishing, pharming and spamming.

Spamming is nothing but sending unsolicited bulk and/or commercial messages over the internet to various users across the globe. Spam mails clog the network of the service provider, thereby interfering and disrupting the services to the users. Spam mails not only exhaust the limited resources of the user/ consumer but also put financial strain on the service provider.

As per International Telecommunication Union (ITU), "although there is no a single solution to overcoming spam, appropriate legislation and effective enforcement are two of the main elements in the fight to combat the problem. As the phenomenon of spam is relatively recent, not all countries have spam laws, and even those that have already implemented specific legislation are currently facing the problem of enforcement at the national and international level. Furthermore, spammers (often also scammers) are increasingly exploiting the international nature of the Internet. For this reason, cross-border cooperation is crucial both in the elaboration and the implementation of new legislation and in its subsequent enforcement." [1]

Further, Sec.66 of the said Act has been amended to cover computer related offences. The proposed amendments to Sec.66 are as follows:

"66. Computer related offences:

a) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource

(i) accesses or secures access to such computer resource;

(ii) downloads, copies or extracts any data, computer data base or information from such computer resource including information or data held or stored in any removable storage medium;

(iii) denies or causes the denial of access to any person authorised to access any computer resource;

he shall be punishable with imprisonment upto one year or a fine which may extend up to two lacs or with both;

(b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource

(i) introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;

(ii) disrupts or causes disruption or impairment of electronic resource;

(iii) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer resource;

(iv) provides any assistance to any person to facilitate access to a computer resource in contravention of the provisions of this Act, rules or regulations made thereunder;

(v) damages or causes to be damaged any computer resource, date, computer databse, or other programmes residing in such computer resource;" [2]

However, it fails to cover acts relating to misrepresentation on the internet, which may lead users to transfer their personal data at their own will. Such acts which are known as phishing and pharming are not adequately covered in the proposed amendments. The criminals/offenders in such cases host a website with distinctively similar domain name and the websites with similar look and feel as compared with original website of the company. The consumer/ user thinking that he is logging on to the companies website passes his information, which is captured by criminals/ offenders. Such offences are different from hacking, unauthorised access or tampering etc. and are related to misrepresentation and passing off. There may not be direct financial loss to the consumer/ user, thereby making it difficult for the authorities to prosecute the offender under the Information Technology Act.

Today, when most of the developed countries are amending their existing legislations, adopting

new legislation to curb and control spamming, phishing and pharming, it most advisable that India should also adopt adequate provisions to prosecute offenders in such cases. The legislation should be amended so as to cover technological changes and related offences.

References

[1] International telecommunications Union at http://www.itu.int/osg/spu/spam/law.html viewed in February 2006.

[2] Ministry of Information Technology, Government of India, http://www.mit.gov.in/itact2000/ITAct.doc viewed in January 2006